White Paper

Evaluating Cloud File Sharing and Collaboration Solutions

By Terri McClure, Senior Analyst

August, 2012

This ESG White Paper was commissioned by Accellion, Inc. and is distributed under license from ESG.

Contents

Executive Summary 2

Why Do We Need Online File Sharing and Collaboration? 3

Rampant Consumerization is Changing How We Share and Access Data 3

The Impact of Consumerization 4

Online File Sharing Market Trends 5

Evaluating Solutions 6

Online File Sharing and Collaboration Service Offering Basics 6

Infrastructure Choices 7

Service and Support 8

Administration and Control Capabilities 9

Security and Availability Features 9

The Bigger Truth 11

Executive Summary

Consumerization has had a broad impact on IT—users are bringing in their own devices and subscribing to their own applications without necessarily waiting for IT's permission. Users want and need to be able to access documents from multiple intelligent endpoint devices, so an area ripe for "rogue" application adoption is the file sharing and synchronization space, where users are subscribing to consumer applications like Dropbox to share files between devices and collaborators. This creates a big challenge for IT, which is in charge of managing and protecting corporate information assets, since it has no visibility into or control over what is stored and shared in these consumer solutions. It also introduces challenges around data leakage, as data stored in these applications goes with the application subscriber—and if the application subscriber is the individual employee, when that person leaves the company, the data goes with her!

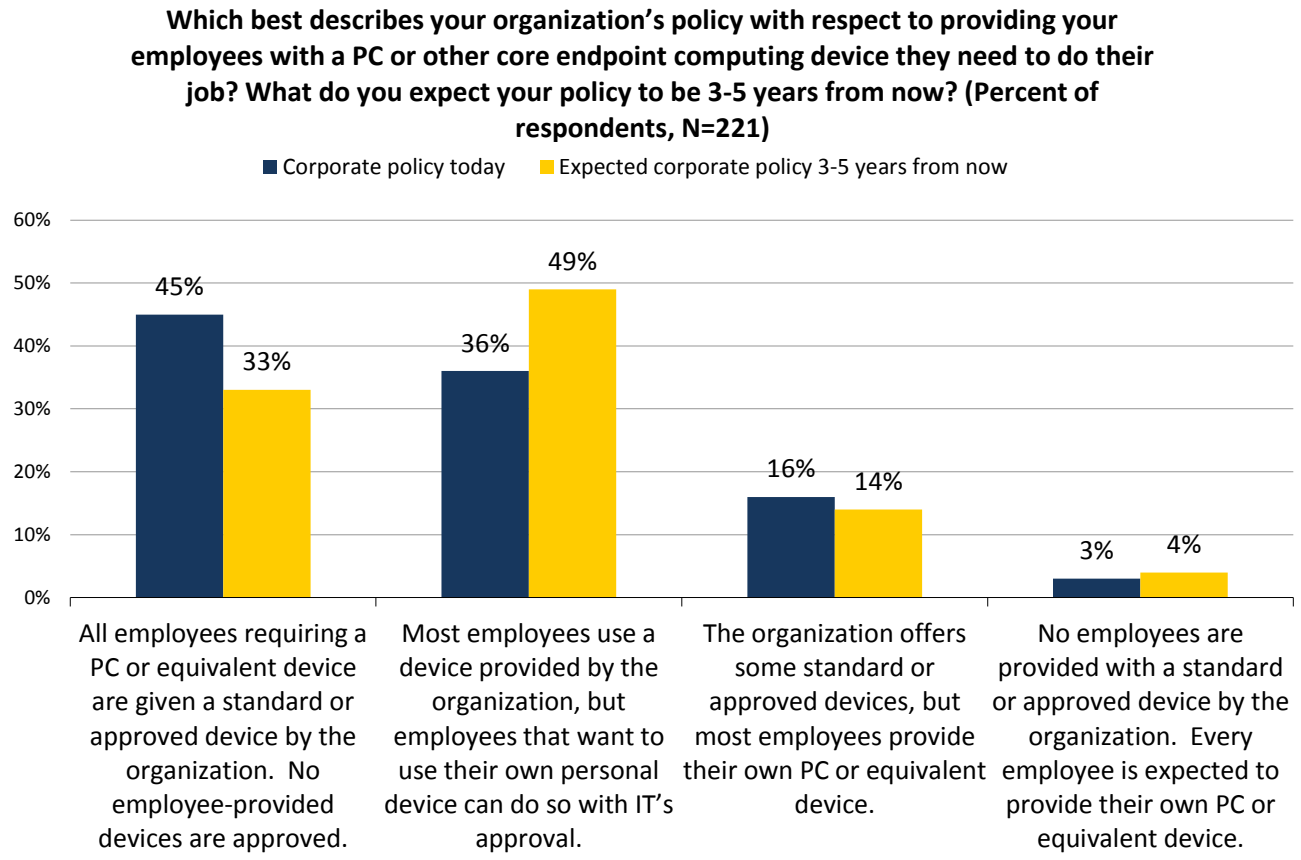
IT is in a defensive position as it needs to try to get back in front of this situation and address data security and administration requirements while also addressing the needs of the mobile workforce. Outlawing these applications is not necessarily the answer. Reducing the friction in sharing files between devices and collaborators can reduce the cost of doing business and speed productivity. There are a number of solutions on the market today that meet a variety of sharing, collaboration and security needs—IT just needs to do its homework and ask tough questions when evaluating solutions. This paper takes a look at the consumerization trends and challenges, and provides a checklist of things IT should be thinking about when evaluating online file sharing and collaboration solutions.

Why Do We Need Online File Sharing and Collaboration?

Rampant Consumerization is Changing How We Share and Access Data

The trend toward "consumerization" marches onward in IT. More and more end-users are choosing their own hardware platforms and software applications in lieu of the IT-sanctioned business tools provided by their companies. In an ESG research study conducted in 2011, 84% of the respondents reported moderate to significant growth in the use of alternative endpoint computing devices.[1] Corporate policies are evolving to support the trend, as 67% of IT organizations expect to be supporting some level of BYOD within the next 3 – 5 years (Figure 1).[2]

Figure 1. Organizations Embrace BYOD



Source: Enterprise Strategy Group, 2011.

The typical end-user has two or more devices—often it is a combination of smartphone, tablet, and laptop. These end-users are looking to tackle issues like data sharing, portability, and access to their data from multiple intelligent endpoint devices, creating a conundrum for IT as it needs to balance business enablement, ease of access, and collaborative capacity with the need to maintain control and security of information assets.

This need for balance is one of the drivers of the fast-growing online file sharing and collaboration market, but only one driver. Perhaps the bigger driver is that there are many consumer-based solutions on the market today that end-users are deploying for personal use and are bringing into the enterprise. These tools pose multiple security risks for IT, the biggest being data leakage. If an employee subscribes to a service on their own, the account belongs to that employee. When the employee leaves, the data goes with them, and IT has no idea what that data may have been. But further issues exist—such as lack of control over corporate data assets and lack of knowledge

[1] Source: ESG Research Brief: *Securing IT Consumerization*, August, 2011.
[2] Ibid

about who is sharing what data with whom—it can get pretty ugly from a security and control standpoint having unauthorized personal file sharing accounts strewn across the enterprise.

The net result is that IT is getting pulled into this space whether it likes it or not. ESG defines the market as:

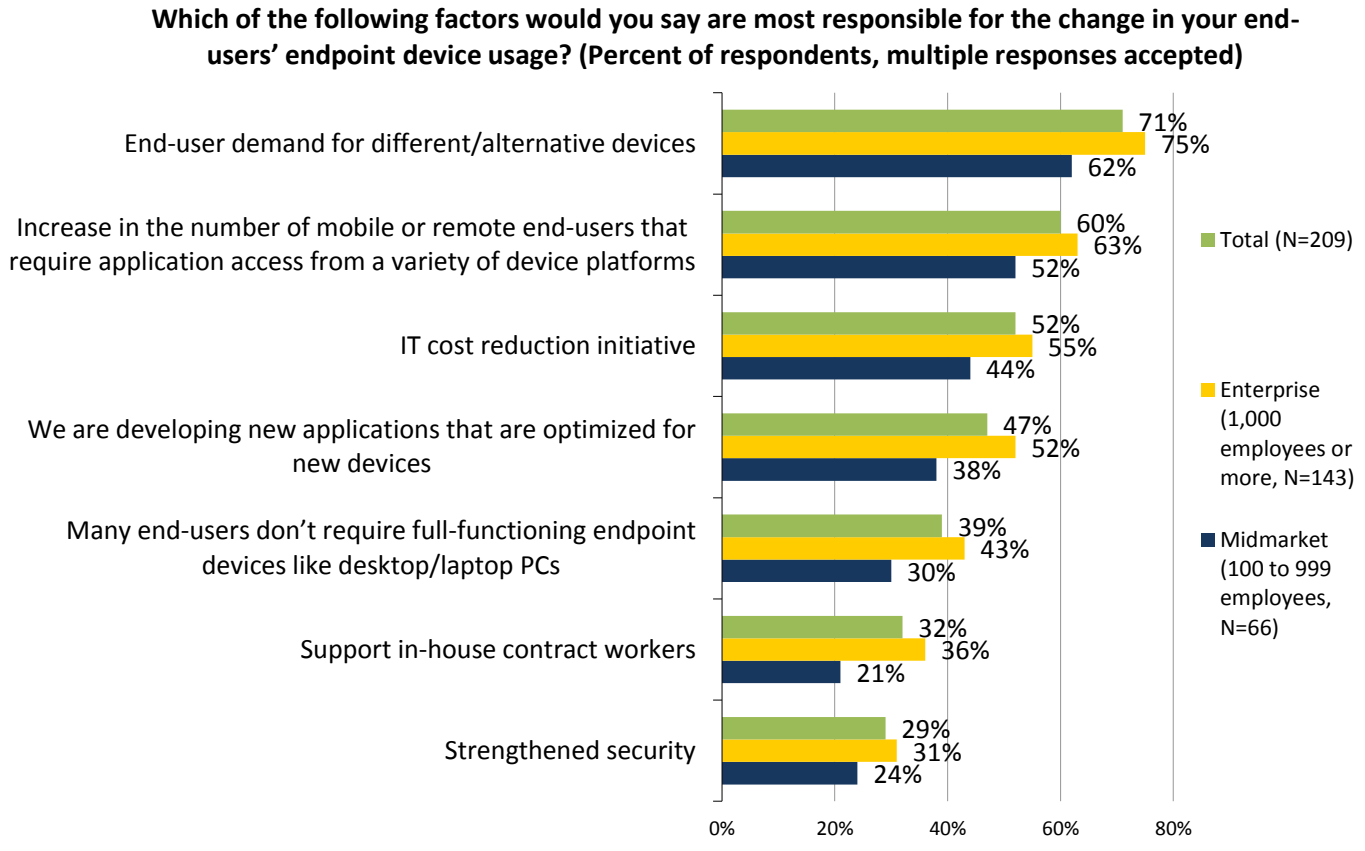
> *Solutions that help users share and access documents stored in either a public, hybrid, or private cloud over the Internet, allowing for easy access by and collaboration across multiple endpoint devices and enhancing mobile user productivity.*

There is a lot to think about when it comes to evaluating which solution might be the right one for an organization. This paper will further examine market dynamics and provide some guidance on what questions you should ask when evaluating solutions.

The Impact of Consumerization

ESG has observed a significant shift in the acceptance of alternative endpoint devices by corporate IT staffs. What are the forces compelling these changes? As shown in Figure 2, end-user demand tops the list of drivers for alternative endpoint device usage, identified by nearly three-quarters (71%) of respondent organizations. The trend is more evident in larger IT shops with more than 1,000 people in the overall organization. With the continued mass market adoption of sophisticated devices like smartphones and tablets in the consumer space, it simply follows that these users would push to utilize those devices for both personal and work purposes. The second most commonly cited factor causing a shift in endpoint computing also involves employee influence, specifically mobile or remote end-users requiring application access from a variety of devices.

Figure 2. Factors Responsible for Change in Endpoint Device Usage, by Company Size



Source: Enterprise Strategy Group, 2011.

As a result of these changes, many organizations are also modifying their policies to accommodate the influx of employee-owned and -provided PCs, tablets, and other endpoint computing devices. For example, of companies

that allow end-users to bring their own PC or equivalent device, 83% allow employees to use the device for both personal and business use. In addition, 54% of companies currently provide a stipend to pay for devices, while another 27% plan to in the future.[3]

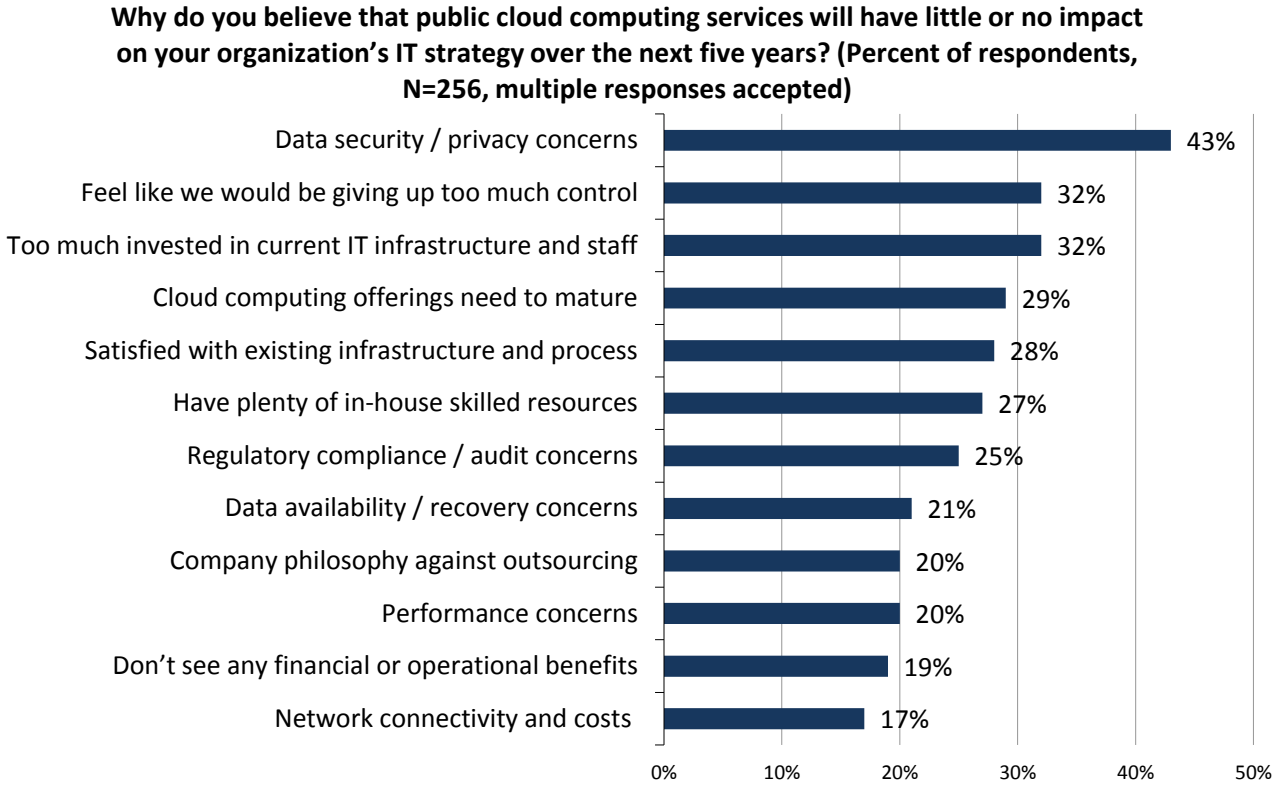
Ultimately, consumerization can be a "win-win"—corporate IT staffs pass on the cost of device acquisition and service plans while maintaining control over their organization's information, and employees have the freedom to use devices of their own choosing. However, there are critical issues that IT managers must consider, such as providing application and workspace deployment options that enable IT to manage and maintain user identity, device independence, security, and predictable productivity. As we will soon discuss, these considerations will be paramount for enterprise IT organizations who not only are facing end-users that want to use popular online file sharing and collaboration solutions, but that want to do so from the endpoint device(s) of their choosing.

Online File Sharing Market Trends

In speaking to both end-users and vendors, one thing is clear: while IT *departments* are not necessarily proactively shopping for new online file sharing and collaboration solutions, IT's *customers*, actual end-users, have adopted these applications in droves for both personal and business use. With cloud applications becoming ubiquitous thanks to their ease of use, fast and easy installation, data protection and portability features, more employees are "going rogue" by using SaaS offerings for both personal *and* business requirements, bypassing their organizations' IT departments at least temporarily, forcing IT to take a look at these applications to "catch up" to users.

This, of course, has huge implications for IT. Many IT executives remain reluctant to embrace SaaS and other public cloud computing services. Indeed, in a survey of senior IT professionals, ESG asked about factors preventing companies from adopting cloud computing services.[4] Figure 3 shows their responses, including the top two inhibitors: security/privacy concerns and loss of control.

Figure 3. Factors Preventing Widescale Adoption of Public Cloud Computing



Source: Enterprise Strategy Group, 2011.

[3] Source: ESG Research Brief, *Corporate Endpoint Device Policies Evolve*, June 2011.
[4] Source: ESG Research Report, *Cloud Computing Adoption Trends*, May 2011.

As a result of their end-users' "rogue" activity with respect to adopting externally-hosted cloud apps, IT organizations are put in a reactive position and have to address security (plus a host of other) concerns to ensure employees are using a secure service and corporate information assets are not placed at risk. Whether they like it or not, IT is ultimately being forced to do their due diligence on new cloud applications so that they can support their end-users' requirements while making an investment in secure, enterprise-ready platforms.

It is no wonder that data security and privacy concerns are top of mind for IT professionals when it comes to evaluating cloud services. Employees have access to all types of confidential information including employee data, customer data, and intellectual property. IT departments do their best to harden networks in efforts to protect this data, but their work is negated if they can't protect or access company data employees are storing in the cloud.

What's more, online file sharing and collaboration applications introduce new challenges as they typically allow users to store and access data via many different devices: desktops, laptops, tablets, smartphones, and any other device with Internet connectivity. IT departments will realize quickly that there needs to be an endpoint device security discussion. What happens when data can walk away with a tablet or cell phone? What policies need to be in place to protect data? Is password protection enough, or does IT need to be able to remotely wipe data from a lost device?

When it comes to traditional file sharing and collaboration solutions, IT generally configures and manages policies that dictate which employees have read/write access to certain files, how often files are backed up/synced, and where files can be accessed from. SaaS applications shift that control to end-users, which can cause issues and headaches for IT in the long run.

Interestingly enough, while cost savings is often cited by cloud vendors as a driver for cloud adoption, ease-of-use and business enablement seem to be bigger drivers for the adoption of online file sharing and collaboration services. ESG talked to a number of end-users who've done head-to-head cost analysis and determined that, for their use cases, buying a dense storage system with high capacity SATA drives and keeping everything in house would actually be cheaper for them. But ease-of-use, the ability to support any endpoint device (with tablets being cited most often) and avoidance of the need for logging into a VPN to even get to a shared drive far outweigh the extra cost of going to the cloud. Additionally, users cited the business agility enabled by capacity on demand as another major benefit that just can't be weighed in a one-to-one cost analysis.

This cloud-based file sharing revolution is driven by users, and IT departments are being dragged in. End-users indicate that they are moving toward new applications and IT service delivery models and away from storing data on classic fixtures like systems from NetApp and EMC or Linux or Windows file servers. As such, expect to see some level of share shift from file servers to online solutions over time, though the biggest near-term impact is likely to be on laptop and desktop drives as more devices with wi-fi, 3G, and 4G support become available. This may trigger users to shift working data that they would normally keep on their PC to the cloud.

Evaluating Solutions

Given the "horizontal" nature of file sharing and collaboration (i.e., effectively every knowledge worker with an Internet-connected device is a potential user), the increasing number of remote and mobile workers in most organizations, and the proliferation of alternative endpoint devices, online file sharing and collaboration represents a natural cloud-based application. Consequently, ESG recommends corporate IT departments get in front of the coming wave of end-users using or demanding use of these services, and endorse a single offering that best balances collaboration and file sharing needs with IT's security and control requirements. With a smart and educated investment, companies stand to satisfy their users while enjoying better security and control over company information, better administrative capabilities, and ultimately, peace of mind.

Online File Sharing and Collaboration Service Offering Basics

Pricing and offerings differ based on the amount of storage, number of users, levels of support, and availability of data on mobile devices. IT departments should pay particular attention to scalability (licensing structures and how easy it is to add users) and SLAs (whether there is an uptime guarantee). Users need to be careful—it can be

difficult to do an apples-to-apples pricing comparison because some charge per seat, some have capacity limits or charge by capacity, and some custom quote pricing for business users. This is, indeed, a nascent market and offerings will likely continue to evolve as vendors evaluate pricing models and make land grabs with attractive pricing options designed to lure users.

Users don't need all of these features – the biggest step for IT to take is to evaluate the departmental requirements for file sharing and collaboration to understand workflow requirements and scope.

- ✓ **Base Functionality checklist**
  - What are the basic services the solution provides?
    - Does it sync data across endpoint devices for offline access? Do you need sync—will employees require access to all their files while they are offline?
    - Does it cache data to offline devices? Few solutions automatically sync to all devices—this is especially true when it comes to tablets and smartphones that have limited capacity such that users would not want all their files chewing up space on these devices. But many solutions will allow users to selectively cache or "favorite" files for offline access as needed.
    - Does it allow easy sharing of files between employees? Outside the company?
    - Can users easily search for files across their synced directory trees?
    - What type of collaboration features does it support? Is there workflow or check in/check out functionality?
    - Does the system support versioning? Do versions expire after a set time period? How many versions are saved? Again, solutions are all over the map on this one. Some save unlimited versions but only for 30 days, some save only up to five versions, some have configurable version depth, and some don't version at all!
  - How broad is the endpoint device support?
    - Most solutions support Android and iOS platforms as well as Windows, but it is important to know your audience and ensure the breadth of endpoint device support matches your breadth of requirements. There are still many emerging solutions on the market that may not meet your needs.
  - Are there file size limits that could prohibit storing and sharing your corporate data?
    - Understand the characteristics of the data sets employees will be sharing. Many services have file size limits to assure quality of service, but that can limit usability if you have larger files!
- ✓ **Pricing Models**
  - Is pricing seat-based, capacity-based, or some combination of both? What are the capacity limits, and are they flexible?
  - How are features such as enterprise application integrations priced? Are there chargeable add-ons?

Infrastructure Choices

While this paper has largely focused on cloud-based services, there are a number of enterprise software offerings on the market today that allow IT to deploy online file sharing solutions on premises, behind the firewall, but leverage the Internet for data access and sharing via mobile clients. The market is evolving quickly and there are offerings available to meet a wide variety of deployment criteria.

Public Cloud Service Providers

It is important to understand on what infrastructure the service provider is storing your data—this is especially important when evaluating SLAs, as we will cover in the next section. When it comes to online file sharing and collaboration public cloud services providers, there are four levels of infrastructure commonly found. These are:

1. The service provider owns the data center and all the technologies and people, like the Amazon, Google, IBM and Oracle models.
2. A co-location model where the service provider rents the physical space from a Tier A Data Center provider but owns hardware, storage, software, and its own people manage the data center operations.
3. A lease model where the service provider rents the physical space and hardware but runs its own software on it.
4. Use Amazon and outsource everything.

✓ **Deployment Model Checklist**

- Public cloud-based service? What is the underlying infrastructure? Who is responsible for the SLAs?
- Hybrid? What is the underlying infrastructure for the service provider portion? Who is responsible for the SLAs?
- On premises? What are the hardware requirements? Who qualifies hardware? What limitations are there on my hardware choices?

Service and Support

With varying ownership models we also see varying service levels available. In addition, those making the shift from traditional storage vendors to the online space should be warned: chances are they are used to a certain level of support and while some vendors offer "premium" or "dedicated" support options, others only offer FAQs and online help.

At first glance, many offerings may seem similar. However, there are differences in terms of which vendors/service offerings are better suited to enterprises and which are better tailored for SME companies. Some offer limited e-mail support and no phone support. Some offer extensive mobile device support, and, in addition to a dedicated account manager, peace of mind with a 99.9% SLA and 24/7 phone support.

✓ **Support Checklist**

- What service levels are offered? Is there a 24 x 7 option?
- Phone or e-mail support?
- What are the response times?
- Is there an SLA?
  - What is it?
  - Who is responsible for maintaining the SLA?
  - Are there remedies in place if the SLA is not met?

In addition to protecting data from external attacks, users—especially enterprise IT groups—need to be able to access their data. That is where availability capabilities and SLAs (service level agreements) come into play. The question of SLAs can be tricky when subscribing to an online file sharing and collaboration service. Many service providers, especially those that are reliant on Amazon S3, "pass through" the SLA from Amazon, so Amazon is a hidden third party in the contract for services but responsible for maintaining the SLA and providing remedies. That can get murky in the event of an outage that causes a significant business disruption.

Administration and Control Capabilities

In addition to basic file sharing functionality, IT shops looking to roll out online file sharing and collaboration solutions across the enterprise need central administration capabilities for configuration and management tasks. Since this is not a requirement for consumer solutions, ESG finds that most vendors are still building out their capabilities in this area. These are critical requirements, however, and the service providers that make it easy for IT to implement and manage their solutions will have a natural edge over the competition.

Among the key administration and control questions that enterprise customers should ask are:

✓ **Administration and Control Checklist**

- Can group policies be set from a central dashboard, or does each account need to be set individually?
- Is there integration with Active Directory for not just Single Sign-On to the service but also, leveraging Active Directory Groups for fast and easy provisioning, de-provisioning, and policy management?
- Does the offering allow for administrator visibility into account usage and file sharing through audit reports and provide data for chargebacks to business units?
- Is there a search capability that allows administrators to find files across the entre domain?
- Are there blacklists and whitelists that allow for setting policies about what domains users can share data with?
- Can IT set sharing and collaboration policies such as what data can be shared outside the company?
- Are there user and group quotas to ensure no one is using an inordinate amount of the available capacity?
- How easy is it to de-provision accounts?

Security and Availability Features

As previously mentioned, security is the number one concern when it comes to enterprise IT's adoption of cloud services. Clearly, there are many security considerations when it comes to sharing and accessing company data via online file sharing services. For example, where employees have access to sensitive data through consumer devices, the risk of a data breach increases and could result in the loss or theft of intellectual property, compliance violations, and costly disclosure and remediation payments. In addition, companies within regulated verticals need to weigh requirements such as HIPAA compliance or Safe Harbor certification more heavily when considering a solution.

Companies with a high number of remote workers or employees that use mobile devices for business need to be aware that compromised consumer devices could be used to launch a broader attack. Since devices are often owned by employees, they may not have security software installed, putting both the data and the company at risk.

Outsider attacks can also target the service provider's data centers as well. Enterprise customers considering any online file sharing and collaboration service should ask service providers detailed questions regarding their information security and physical security controls and processes, including the degree to which they adhere to a secure software development methodology.

IT professionals should remember, however, that aside from regulated or IP data, there is a huge amount of unstructured data that is not sensitive or suitable to be heavily guarded under lock and key. One of the biggest issues will be determining what types of data are okay for mobility.

✓ **Security Checklist**

- Is data encrypted in flight and at rest?

- Where are the encryption keys held?
  - Many service providers hold encryption keys to enable frictionless sharing within and between domains. Typically the keys are stored in a separate data center than the one in which the data is held, so hacking into user files would require breaking into two data centers. Few solutions allow the keys to be held within the corporate data center. Those are typically private or hybrid cloud solutions providers but some emerging vendors do this as well.
- Is there remote "wipe" capability that allows an administrator to erase the corporate folders in the event a device is lost or an employee leaves the company?
- Is the data center SAS 70 type 2 certified?
- Is there integration with mobile device management solutions?
- Is the data center HIPAA, PCI, FINRA or Safe Harbor (add your regulatory body name here) certified?

Another key area to consider from a management standpoint is the vendor's data protection and redundancy. Just how safe is user data in the event of a hardware failure? A site failure? How many versions are available for recovery? Service provider offerings run the gamut, with some having limited or no real disaster recovery capability and just local hardware redundancy and others supporting multiple remote disaster recovery sites as well as local redundancy. Users need to consider business continuity when they standardize on a service provider—if data is inaccessible for a period of time, how much will that impact the business? If the answer is "it won't," any solution will meet the need, but if there are big time business costs associated with data inaccessibility, then users need to consider a service with multi-site redundancy. Most also have unlimited version history so older versions of documents can be recovered, but with varying degrees of difficulty to get at older versions. If version history and tracking are important, it is worth evaluating these systems for ease-of-use in recovering versions.

A larger company with its own data centers may find it is better served to deploy an on-premises solution and manage its own data protection and recovery if it already has robust policies, procedures, and infrastructure in place.

✓ **Availability Checklist**

- Is the service provider storing your data in a single data center or multiple data centers?
- What are the data center backup and contingency plans?
  - How is data protected? Is there local protection like RAID or mirroring? How many copies of the data are there?
  - Is data replicated remotely to ensure no loss in the event of a site failure?
  - Is there automatic failover to the disaster recovery site in the event of a site failure?
  - How long will failover take?
- Does the system support versioning? How many versions are kept? Is there a time limit under which versions expire? Is the depth of versioning configurable?
  - This was discussed as a basic function but t is also core to data availability and data protection strategies—if versioning is supported and configurable, the file sharing and collaboration solution could provide sufficient levels of data protection to supplant backup.
- Can users perform a self-service restore?

The Bigger Truth

Consumerization is not going away. IT can't continue demanding that everyone have a Windows-based laptop or PC, log into a VPN, and deal with the resulting latency and connectivity issues of remotely logging into a shared file system. This market will only get bigger. Consumerization is driving these solutions, and consumers are driving business adoption. IT is in a defensive position as it needs to try to get back in front of this situation and address security and administration requirements.

While the market started with consumer solutions, corporate IT would be well suited to look at solutions built from the ground up with a pure business use case in mind. The disadvantage for these firms is that they do not have the name recognition that comes with aggressively courting consumers so they are lesser known and hard to find.

No matter how things shape out from a vendor landscape perspective, consumerization and mobility are driving a growing need for online file sharing and collaboration solutions. IT would be well served to get in front of this trend proactively rather than waiting to get dragged in once its users have made their own personal bets on preferred services. Judging by the number of corporate board members that are sitting in board meetings with tablets in front of them using (or needing) these types of solutions, IT will need to have a good solution for secure, enterprise-ready, device-agnostic file sharing and collaboration services sooner rather than later.

Accellion, Inc.

Headquartered in Palo Alto, California, Accellion, Inc. provides enterprise-class mobile file sharing solutions to enable secure, anytime, anywhere access to information while ensuring enterprise security and compliance. More than 10 million users and 1,600 of the world's leading corporations and government agencies including Procter & Gamble; Activision; Indiana University Health; Kaiser Permanente; Lovells; Bridgestone; Ogilvy; Harvard University; Guinness World Records; US Securities and Exchange Commission; and NASA use Accellion to protect intellectual property, ensure compliance, improve business productivity and reduce IT costs.

Accellion offers the industry's widest set of enterprise deployment options including public, private and hybrid cloud deployment and FIPS 140-2 certified environments. All Accellion deployment options can be mixed and matched. Accellion file sharing solutions provide the ease-of-use business users need while giving the enterprise organization the flexibility, scalability and protection it needs.

Accellion mobile file sharing solutions are available for Enterprises, Businesses and Individual Business Users. Accellion secure file sharing capabilities include native Accellion Mobile Apps, kitedrive™ file synchronization, secure workspaces, file commenting, notifications, versioning and secure uploads and downloads. Accellion integrates with Microsoft SharePoint and other enterprise content stores, helping users share files and collaborate externally. In addition, Accellion provides IT with comprehensive management, tracking and reporting tools to ensure enterprise data security and demonstrate compliance with industry regulations such as HIPAA, GLBA and SOX.

For more information on Accellion, Inc. please visit the company's website at www.accellion.com